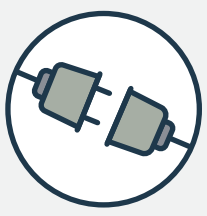
WAS YOUR BUSINESS PHISHED?

What is phishing?

Hackers will send emails disguised as a trusted person or company to your employees. The email might include a link to a scam website that will ask them to input their password or username, allowing the hacker access to your data. The phishing email could also include attachments that, when clicked, install malicious software onto your business network.

If you or an employee clicked on a phishing email, don't panic!

Follow these immediate action steps



Disconnect the computer or device from the Internet/network.

Send a company-wide email notifying employees of the phishing attack.

Run a virus scan on all computers and devices connected to your business network.

Change any compromised passwords right away and enable two factor authentication (2FA) on all of your accounts – which requires an additional code to log in.

Forward phishing emails or websites to the Anti-Phishing Working Group at reportphishing@apwg.org.

If you think a scammer obtained sensitive information, visit IdentityTheft.gov for resources to minimize your business's risk of identity theft.

Cyber Tip

Create a workplace culture where employees don't fear discipline if they accidentally click on a phishing email. Employees should feel comfortable telling management right away. Remember, cybercrime and online fraud can happen to anyone, so use this as an opportunity for you and your employees to learn.

Visit FightCybercrime.org for more recovery resources.

FightCybercrime.org

CybercrimeSupport.org | FightCybercrime.org | ScamSpotter.org